разницей, что для длинных последовательностей никакое сжатие не наблюдается – независимо от соотношения фактической длины последовательности с периодом. Так же, как и для последовательностей двоичных слов генератора Фибоначчи, не наблюдается сжатие двухбайтовых псевдослучайных последовательностей ($N = 3 \cdot 2^{19}$), источником которых был датчик из Mathcad 2003. Это свидетельствует о том, что период датчика $runif$ из Mathcad 2003 очень большой.

Проведенные эксперименты показывают, что последовательности нечётных операндов малой длины (по отношению к длине периода) в некотором смысле симметричны, в частности, остатки этих операндов по модулю четыре повторяются с периодом 4. Представляет интерес исследование асимметрии последовательностей двоичных слов, $L_1 > 0$, содержащих как чётные, так и нечётные числа.

Выводы

Не фильтрованные последовательности операндов, в отличие от подпоследовательностей нечётных операндов, являются достаточно сложными случайными последовательностями. Эти последовательности могут быть приняты в качестве псевдослучайных последовательностей для генерации псевдослучайных чисел (двоичных слов) в силу измерений относительной избыточности, используемых в косвенном критерии оценки псевдослучайности.

*Литература: **1.** O. Goldreich, S. Goldwasser, S. Micali. How to construct random functions//Journal of the ACM, vol.33, E4, Oct 1986, pp.792-807.- kiev-security_org_ua-Криптография_Как построить случайные функции.htm. **2.** В. Мясоедов, В. Куценко, Т. Левченко, Равномерность распределения в шкале наименований. В зб.: Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні.-Науково-технічний збірник.-Вип. 7.-К.:НДЦ "Тезіс" НТУУ "КПІ".-2003.- 224с. - С.179. **3.** В. Мясоедов, В. Куценко, Особенности генерации псевдослучайных чисел. В сборнике „Захист інформації” ... **4.** A. Lempel and J. Ziv, On the Complexity of Finite Sequences, IEEE Trans. on Information Theory Vol. IT -22, Jan. 1976, pp 75-81. **5.** A. K. Leung and S. E. Tavares, Sequence Complexity as a Test for Cryptographic Systems, Advances in Cryptology ’84, pp.75-81. **6.** В. В. Мясоедов, Золотое сечение в шифровании данных. В зб.: Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні.-Науково-технічний збірник.-Вип. 4 .-К.:НДЦ "Тезіс" НТУУ "КПІ".-2002.- 214с. - С. 105.*

УДК 681.5.015: 004.056.57

СИСТЕМА С РАССЕЯННЫМИ ЦИФРОВЫМИ ВОДЯНЫМИ ЗНАКАМИ В УСЛОВИЯХ АТАКИ ФИЛЬТРАЦИЕЙ И АДДИТИВНЫМ ШУМОМ

Ирина Маракова
Одесский национальный политехнический университет

Анотація: **Розглянуто систему с прихованими розсіяними цифровими водяними знаками (ВЗ) з використанням зображень у вигляді головного покриваючого повідомлення в умовах атаки фільтрацією та адитивним шумом. Одержані формули для імовірностей помилок Pm та Pfa як функцій числа елементів ВЗ, постійної перекручень, порогу. Це дозволяє оцінити число потрібних біт ВЗ для забезпечення надійності системи в певних умовах.**
Summary: **We consider private tile-based watermarking (WM) digital system at use as the cover message (CM) of images with additive noise and filtering attack The formulas for probabilities Pm and Pfa are derived as a dependence on the number of WM elements, distortion constraints, chosen threshold. It allows to find out how many bits of WM is necessary to use in order to embed reliable WM for different conditions.**
Ключевые слова: **Водяные знаки, основное покрывающее сообщение, идентификатор.**

I Введение

Основное практическое использование систем с цифровыми водяными знаками (ЦВЗ) – это скрытое или открытое погружение дополнительной идентификационной информации в основное покрывающее сообщение (ОПС) [1, 2]. В простейшем случае декодер такой системы принимает решение о наличии или отсутствии ЦВЗ в ОПС. При этом декодер фактически является обнаружителем (детектором) и система

называется системой с нулевым битом. Представляется интересным рассмотреть простейший алгоритм формирования ЦВЗ с R битами информации, так называемые, рассеянные ЦВЗ [1]. При этом ОПС делится на R фрагментов, в каждый r–ый из которых погружается r–ая компонента ЦВЗ. На основании обнаружения R составляющих ЦВЗ и формируется R битов информации. Аналогичный подход погружения ВЗ использовался при видео ОПС [2]. Исследуется только секретная система, когда ЦВЗ является секретным ключом, известным исключительно легальным пользователям [3]. В приемной части системы используется информированный детектор, которому известно ОПС.

Выполненные в работе теоретические исследования не зависят от вида ОПС (аудио, видео и т. д.), однако, для удобства изложения и при моделировании ОПС считаются изображениями. Для оценки искажений ОПС после погружения ВЗ, которые являются помехой для ОПС, и после воздействия аддитивного шума и преобразования фильтрацией используются отношения сигнал/помеха. Необходимо отметить, что данный параметр оценки искажений ОПС не связан с перцепционной моделью и только косвенно отображает надежность визуального восприятия изображений. Однако, геометрический подход при формировании оценки различий ОПС и стегаобраза (ОПС и ЦВЗ) весьма трудоемок и не имеет однозначных рекомендаций при выборе параметра искажений [4].

Целью нелегального пользователя (атакующего) является изъятие или повреждение ЦВЗ без видимых искажений ОПС. Как правило, для этих целей используются такие преобразования, как добавление аддитивного шума, фильтрация, сжатие и декомпрессия, геометрические преобразования и т. д. В работе рассмотрены атакующие преобразования только в виде аддитивного шума совместно с линейной фильтрацией, менее всего исследованной в литературе [1]. Весьма распространенными являются геометрические преобразования канала атакующего при ОПС изображениях. При масштабировании изображения всего на 2% или вращении на $3{,}5^{o}$ почти на 30 дБ уменьшается пик корреляционной функции исходного и преобразованного изображений [5]. Следовательно, требования надежного визуального восприятия ограничивают интенсивность геометрических преобразований. С другой стороны, результаты исследований эффективности систем с ВЗ в условиях аддитивного шума и преобразований фильтрацией можно рассматривать в качестве нижней оценки. Известны исследования эффективности систем с ЦВЗ с асимптотической оценкой вероятностей ошибок декодера, т. е. при длине ЦВЗ, стремящейся к бесконечности, что на практике не приемлемо [6]. Теоретический анализ устойчивости систем с ЦВЗ к преобразованиям фильтрацией и воздействию аддитивного шума может выполняться на основе оценки пропускной оценки канала [7]. Применяется методика, позволяющая получать аналитические оценки вероятностей ошибок декодера системы, связанные с основными параметрами системы, а именно, длиной и интенсивностью ЦВЗ, параметрами искажений [8, 9].

II Исследование системы с рассеянными ЦВЗ в условиях атаки фильтрацией и аддитивным шумом

Эффективность системы с ЦВЗ с нулевым битом определим посредством вероятностей ошибок

$$P_m=1 - P_c=P(w'=0, w =1), \quad (1)$$

$$P_{fa}=1 - P_o=P(w'=1, w =0), \quad (2)$$

где P_m – вероятность пропуска ЦВЗ; P_c – вероятность правильного обнаружения ЦВЗ; P_{fa} – вероятность ложного обнаружения ЦВЗ; P_o – вероятность правильного не обнаружения ЦВЗ; w' – принятые ЦВЗ; w – погруженные в ОПС ЦВЗ.

В случае погружения R-мерного вектора идентификационных данных (1), (2) преобразуются к векторному виду и эффективность систем будет характеризоваться векторами вероятностей ошибок $\overline{P}_{fa} = P_{fa}^1,\ldots\ P_{fa}^r,\ \ldots,\ P_{fa}^R$ и $\overline{P}_m = P_m^1,\ldots\ P_m^r,\ldots P_m^R$.

В кодере формируется стегасообщение

$$s(\overline{n}) = c(\overline{n}) + w(\overline{n}), \quad (3)$$

где $s(\overline{n}),\ \overline{n} = 0,\ 1,\ldots N$ – стегасообщение; $c(\overline{n})$, $n = 1,\ 2,\ldots N$ – ОПС; $w(\overline{n}),\ \overline{n} = 1,\ 2,\ldots N$ – ЦВЗ; $\overline{n}$ – дискрет во временном пространстве (пиксель при ОПС изображении), $\overline{n} = 1,2,\ldots,N,\ \overline{n} = n_1 n_2$, $n_1 = 1,\ 2,\ldots,\ N_1$, $n_2 = 1,\ 2,\ldots,\ N_2$, $N=N_1N_2$ – длина ОПС и ЦВЗ (для упрощения формул полагаем длину ОПС равную длине ЦВЗ, подразумевая несуществующие члены ЦВЗ нулевыми), N_1 — число пикселей в столбце, N_2 – число пикселей в строке.

Рассмотрим простейший сценарий погружения R битов информации с ЦВЗ, когда ОПС разбивается на фрагменты соответствующего размера, в каждый из которых и погружаются свои ЦВЗ, являющиеся

случайной последовательностью. Общая случайная последовательность ЦВЗ $w(\bar{n})$ является конкатенацией всех R составляющих

$$w_r(\bar{n}) \in w(\bar{n}) = \alpha(-1)^{a_{\left[\frac{\bar{n}}{r}\right]}}, \ r = 1, 3, \ldots R, \ \bar{n} \in A_n, \ \bar{n} = 0, 1, \ldots N, \tag{4}$$

где $\alpha > 0, \ \bar{a} = (a_n))_{\bar{n}=1}^{\frac{N}{r}}$ – последовательность равномерно распределенных нулей и единиц {0,1}, $r > 1$, $\left[\frac{\bar{n}}{r}\right]$ – целые части частного.

Длина каждого r–го ЦВЗ определяется как минимально возможная для обеспечения заданного уровня вероятностей ложного обнаружения P_{fa}^r и пропуска P_m^r ЦВЗ.

Без потери общности исследований в качестве ОПС рассмотрены изображения при числе пикселей N, расположенных на двумерном пространстве.

При атаке в виде аддитивного шума и фильтрации

$$s'(\bar{n}) = s(\bar{n}) * h(\bar{n}) \ + \varepsilon(\bar{n}), \quad \bar{n} \in A_N = 1, \ldots, N, \tag{5}$$

где $h(\bar{n})$ – импульсная характеристика фильтра; * – знак операции свертки стегасообщения $s(\bar{n})$ и импульсной функции фильтра $h(\bar{n})$; $\varepsilon(\bar{n})$ – аддитивный шум атаки.

Критериями качества являются параметры искажения, а именно, отношение сигнал/шум после погружения ВЗ

$$\frac{\mathrm{var}(c(\bar{n}))}{\mathrm{var}(s(\bar{n}) - c(\bar{n}))} \geq \eta_w, \tag{6}$$

и отношение сигнал шум после воздействия аддитивного шума и преобразования линейной фильтрацией

$$\begin{aligned} \frac{\mathrm{var}(c(\bar{n}))}{\mathrm{var}(s'(\bar{n}) - c(\bar{n}))} &= \frac{\mathrm{var}(c(\bar{n}))}{\mathrm{var}((s(\bar{n}) * (h(\bar{n}) - \delta(\bar{n})) + \varepsilon(\bar{n})) - c(\bar{n}))} = \\ &= \frac{\mathrm{var}(c(\bar{n}))}{\mathrm{var}(c(\bar{n}) * (h(\bar{n}) - \delta(\bar{n}))w(\bar{n}) * h(\bar{n}) + \varepsilon(\bar{n}))} \geq \eta_a, \end{aligned} \tag{7}$$

где var(x) – дисперсия случайной величины x; $\delta(1) = 0, \quad \delta(\bar{n}) = 1, \ \bar{n} = 2, \ldots, N$; η_w – отношение сигнал/шум после погружения ЦВЗ в ОПС; η_α – отношение сигнал/шум после атаки на стегосообщение.

Поскольку в модели предполагается, что ОПС, ЦВЗ и шум атаки являются стохостическими независимыми процессами, то

$$\frac{\mathrm{var}(c(\bar{n}))}{\mathrm{var}(c(\bar{n}) * (h(\bar{n}) - \delta(\bar{n})) + \mathrm{var}(w(\bar{n}) * h(\bar{n})) + \mathrm{var}(\varepsilon(\bar{n}))} = \eta_a. \tag{8}$$

В качестве детектора используется наиболее удобный для теоретического анализа линейный корреляционный детектор.

Информированный детектор, которому известна информация об ОПС, формирует для каждого r–го ЦВЗ $w_r(\bar{n})$ величину Λ^r и сравнивает с заранее выставленным порогом λ. Величина порога λ определяется в зависимости от требуемого уровня вероятностей ошибок (1), (2). Если $\lambda \geq \Lambda^r$, то принимается решение о присутствии ЦВЗ в $s'(\bar{n})$, а если $\lambda < \Lambda^r$, то принимается решение об отсутствии ЦВЗ в $S'(n)$.

Для коррелированного линейного детектора

$$\Lambda^r = \sum_{\bar{n} \notin A_N} (s'(\bar{n}) - (c(\bar{n}) * h(\bar{n}))(w_r(\bar{n}) * h(\bar{n}))), \tag{9}$$

в случае погруженного ЦВЗ

$$\Lambda^r = \Lambda_1^r = \sum_{\bar{n} \in A_N} [w_r(\bar{n}) * h(\bar{n}) + \varepsilon(\bar{n}))(w_r(\bar{n}) * h(\bar{n})], \tag{10}$$

и, если в стегасообщении ЦВЗ отсутствуют,

$$\Lambda^r = \Lambda_0^r = \sum_{\bar{n}\in A_N} \varepsilon(\bar{n})(h(\bar{n}) * w_r(\bar{n})). \tag{11}$$

Поскольку ЦВЗ выбирается случайным образом, то в соответствии с центральной предельной теоремой ааналитические оценки вероятностей ошибок

$$P_m^r = 1 - Q\frac{(\lambda - E(\Lambda_1^r))}{\sqrt{\mathrm{var}\,\Lambda_1^r}}, \tag{12}$$

$$P_{fa}^r = Q\frac{\lambda - E(\Lambda_0^r)}{\sqrt{\mathrm{var}\,\Lambda_0^r}} \tag{13}$$

где $Q(x) = 1/\sqrt{2\pi}\ \int_x^\infty e^{-\frac{t^2}{2}}dt$.

Без потери общности исследований положим $E(\varepsilon(\bar{n})) = 0$, тогда

$$E(\Lambda_0^r) = 0 \tag{14}$$

и в соответствии с (10)

$$E(\Lambda_1^r) = E\sum_{\bar{n}\in A_N}((w_r(\bar{n}) * h(\bar{n}))^2 = \sum_{\bar{n}\in A_N} E\sum_{n_1=1}^{N_1}\sum_{n_2=1}^{N_2} w_r(n_1)w_r(n_2)h\ (\bar{n}-n_1)h(\bar{n}-n_2) =$$
$$= \sum_{\bar{n}\in A_N}\sum_{n_1=1}^{N_1}\sum_{n_2=2}^{N_2}\psi_{w_r}(n_1,n_2)h(\bar{n}-n_1)h(\bar{n}-n_2) \tag{15}$$

где $\psi_{w_r}(n_1,n_2) = E(w_r(n_1)w_r(n_2))$ – корреляционная функция *r*–го ЦВЗ; для простоты предполагается, что отдельные составляющие ЦВЗ характеризуются одинаковыми вероятностными мерами.

Если рассмотреть сценарий, когда ЦВЗ и аддитивный шум атаки являются некоррелированными последовательностями и

$$\psi_{w_r}(\bar{k}) = \alpha^2, \quad \bar{k} = 1,..., N, \tag{16}$$

то можно найти

$$P_m^r = 1 - Q(\lambda' - \mu), \tag{17}$$

$$P_{fa}^r = Q(\lambda'), \tag{18}$$

где

$$\lambda' = \frac{\lambda}{\sqrt{\mathrm{var}(\Lambda^r{}_0)}} = \frac{\lambda}{\alpha\sigma_\varepsilon\sqrt{\sum_{k=1}^N\left|\hat{h}(\bar{k})\right|^2}}, \tag{19}$$

$$\mu = \frac{E(\Lambda_1^r)}{\sqrt{\mathrm{var}(\Lambda_0^r)}} = \frac{\alpha}{\sigma_\varepsilon}\sqrt{\sum_{k=1}^N\left|\hat{h}(\bar{k})\right|^2} \tag{20}$$

σ_ε^2 – дисперсия аддитивного шума атаки; $\hat{h}(\bar{k})$ – частотная характеристика линейного фильтра.

Рассмотрим некоторое ОПС со спектром

$$\psi_c(\bar{k}) = \frac{1}{\sigma_c^2}\sum_{\bar{n}=1}^N \psi_c(\bar{n})e^{-j2\pi k\frac{\bar{n}}{N}}, \qquad \bar{k} = 1,..., N, \tag{21}$$

($\psi_c(\bar{n})$ – корреляционная функция ОПС; $\sigma_c^2 = \mathrm{var}(c(\bar{n}))$ – дисперсия ОПС) и используем в качестве фильтра идеальный фильтр нижних частот (ФНЧ)

$$\hat{h}(\bar{k}) = \begin{cases} 1, \ \textit{если}\ 0 \le \bar{k} \le K_h, \\ 0, \ \textit{в других случаях} \end{cases}, \tag{22}$$

где $0 \le K_h \le N-1$, K_h – относительная частота среза.

На основе (21), (22) представим (7) в виде

$$\frac{\sigma_\varepsilon}{\alpha} = \sqrt{\frac{\eta_w}{\eta_\alpha} - \frac{1}{N}\sum_{k=1}^{N}\left|\hat{h}(\bar{k})\right|^2 - \frac{\eta_w}{N}\sum_{k=1}^{N}\left|h(\bar{k})\right|^2 \psi_c(\bar{k})}\,. \qquad (23)$$

Таким образом, предоставляется возможным выполнить количественную оценку вероятностей ошибок $\overline{P}_{fa} = P_{fa}^1,\ldots P_{fa}^R$ и $\overline{P}_m = P_m^1,\ldots P_m^R$, используя (17 – 20) и (23) для конкретных параметров системы, а именно: частотной характеристики фильтра атаки $\hat{h}(\bar{k})$, спектральной плотности ОПС $\psi_c(\bar{k})$, количества элементов ЦВЗ N_r, параметров искажений η_w и η_α.

Поскольку оценка спектральной плотности реального ОПС $\psi_c(\bar{k})_{\bar{k}=1}^{N}$ является весьма сложной задачей, далее будем исходить из того, что фильтр атаки должен выбираться из условия минимальных искажений ОПС. С этой точки зрения предположим, что последнее слагаемое в (23) пренебрежительно мало, тогда

$$\frac{\sigma_\varepsilon}{\alpha} = \sqrt{\frac{\eta_w}{\eta_\alpha} - \frac{1}{N}\sum_{\bar{k}=1}^{N}\left|\hat{h}(\bar{k})\right|^2}\,. \qquad (24)$$

Подставив (21) и (24) в (20) и учитывая (4), получим

$$\mu = \sqrt{\frac{K_h}{(\eta - \frac{K_h}{N})R}} = \sqrt{\frac{KN}{(\eta - K)R}}\,, \qquad (25)$$

где $K = \frac{K_h}{N}$, $\eta = \frac{\eta_w}{\eta_\varepsilon}$.

При отсутствии атаки фильтрацией $(K_h = N)$

$$\mu_o = \sqrt{\frac{N}{(\eta - 1)R}}\,. \qquad (26)$$

На основе (26) можно сделать вывод, что использование рассеянных ЦВЗ в R раз ухудшает эффективность системы по сравнению с эффективностью системы с нулевым битом.

Анализируя выражения (25), (26), можно сделать заключение, что атака фильтрацией ухудшает эффективность систем с рассеянными ЦВЗ. Для обеспечения некоторого уровня вероятностей ошибок при наличии атаки фильтрацией по сравнению с системой без атаки фильтрацией потребуется увеличить исходную длину ЦВЗ N в $\frac{1}{K_h}$ раз. Однако, если атакующий применяет в качестве аддитивного шума атаки $\varepsilon(\bar{n}) = \varepsilon'\left(\left[\frac{\bar{n}}{R'}\right]\right)$ и $R' < R$, где R определяется (5), то всегда представляется возможным для любого значения относительной частоты среза K_h подобрать такое значение параметра R, чтобы искажения ЦВЗ посредством фильтрации сводились к минимуму. То же верно при $R' > R$.

III Иллюстрация результатов и выводы

Исследуем влияние атаки фильтрацией при использовании рассеянных ЦВЗ в частном случае, когда $w(\bar{n})$, $\varepsilon(\bar{n})$ – некоррелированные последовательности. Было выбрано ОПС в виде фактурного изображения, в которое аддитивно погружались ЦВЗ в соответствии с (2). Атакующая модель фильтра соответствует (5), где

$$h(\bar{n}) = \frac{1}{U}e^{-\frac{n_1^2+n_2^2}{2\delta^2}},\ U = \sum_n e^{-\frac{n_1^2+n_2^2}{2\delta^2}}\,. \qquad (27)$$

На рис. 1 представлены зависимости $N = f(\delta)$ при $\eta = \eta_w / \eta_\alpha = 2$ для двух различных рассеянных ЦВЗ (R = 2, R = 5) и при фиксации вероятностей ошибок не более $c = \bar{n}$. Рассмотрен только один

сценарий: атака фильтрацией и аддитивным шумом, $w(n)$ – некоррелированная последовательность типа (4), $\varepsilon(n)$ – некоррелированная последовательность с нормальным распределением и нулевым средним. При параметре ФНЧ $\delta = 0{,}7$ для обеспечения эффективности системы не менее заданного уровня $P_m^r = P_{fa}^r \geq 10^{-3}$ при $R = 2$ потребовалось $N \geq 240$ и при $R = 5$ – $N \geq 600$ ($N \geq 120$ при $R = 1$).

При использовании в качестве ЦВЗ коррелированных последовательностей следует ожидать некоторое улучшение эффективности системы при атаке линейной фильтрацией и аддитивным не коррелированным шумом. Однако, при использовании атаки коррелированной помехой наряду с атакой линейной фильтрацией данный выигрыш будет уменьшаться [8].

Получены формулы для оценки вероятностей ошибок P_m^r, P_{fa}^r при атаке аддитивной помехой и линейной фильтрацией и использовании линейного корреляционного детектора. Показано, что даже если атака существенно не изменяет качества ОПС, эффективность системы ухудшается, если ЦВЗ является некоррелированной последовательностью.

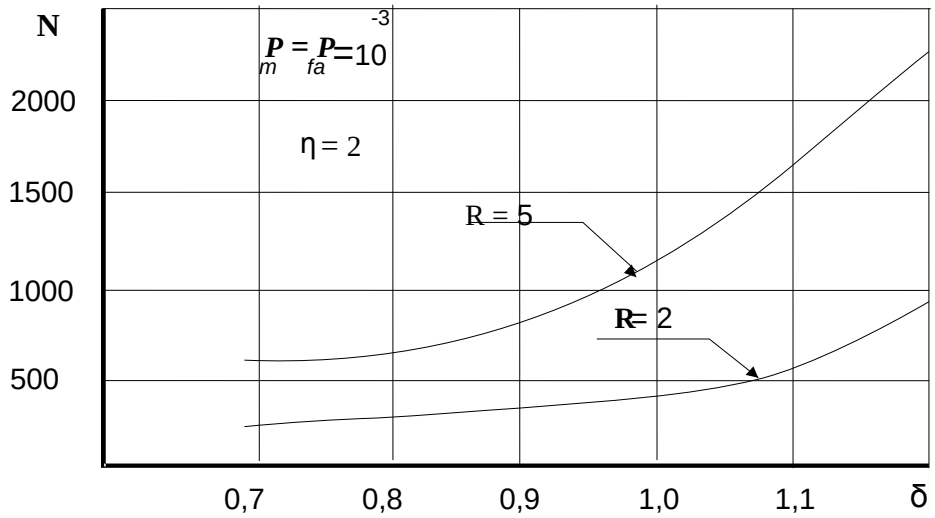

Рисунок 1 – Зависимость $N = f(\delta)$ при фиксированных параметрах η, m, α, заданном уровне вероятностей ошибок $P_m = P_{fa}$ и при использовании в качестве ЦВЗ и аддитивной помехи некоррелированных случайных последовательностей

Теоретические результаты подкреплены моделированием, которое продемонстрировало существенное ухудшение эффективности при атаке фильтрацией даже в том случае, когда качество стегасообщения особо не страдало. Использование рассеянного ЦВЗ при атаке фильтрацией является предпочтительным с той точки зрения, что появляется дополнительная возможность улучшать эффективность системы посредством подбора параметра R для (4).

Другими словами, если ОПС обработано ФНЧ с частотным откликом, близким к (22), то при отсутствии видимых ухудшений качества ОПС эффективность системы ЦВЗ ухудшится в rN_r / K_h раз, где N_r – длительность r–ой составляющей ЦВЗ. Этот результат хорошо согласуется с положением теории широкополосных систем связи.

Однако, ряд вопросов остается открытым. В частности, построение оптимального приемника, когда ЦВЗ декодеру не известны частотная характеристика атакующего фильтра. С другой стороны, применение более совершенных алгоритмов кодирования вне сомнения позволит улучшить основные параметры системы с ЦВЗ.

Литература: ***1.*** *S. Katzenbeisser, F. Petiticolas. Information Hiding. – N. Y.: Artech House Inc., 2000, 270 p.* ***2.*** *Kutter M., Jordan F., Bosses F. Digital Signature of Color Images Using Amplitude Modulation // Proc. of the SPIE Storage and Retrival for Image and Video Databased, Vol. 3022, USA, California., 1997. P. 518 – 526.* ***3.*** *Маракова И. И., Сафронов А. С. Проблематика и перспективы развития методов сокрытия информации // Труды*

Одесск. политехн. Университета, 2003, вып. 1(19), С. 184–188. ***4****. Basri R. Recognition by Linear Combinations of Models // IEEE Trans. on Pattern Analysis and Machine Intelligence., 13(10, 1991, P. 992 – 1006.* ***5****. Lin C. Y., Wu M., Bloom J. A., Cox I. J., Miller M. L ., Lui Y. M. Rotation, Scale and Translation Resilient Watermarking for Images // IEEE Trans. On Image Processing, Vol.10(5), 2001, P. 767 – 782.* ***6****. J. K. Su, J. J. Eggers, B. Girod. Analysis of Digital Watermarks Subjected to Optimum Linear Filtering and Additive Noise// Signal Processing.. Vol.81(1). 2001. P. 1141— 1175.* ***7****. Moulin P., O'Sullivan J. Information Theoretic Analysis of Information Hiding // Proc. IEEE Symp. on IT' 1998, P. 147–183.* ***8****. Маракова И. И., Мараков Д. А. Методика оценки эффективности систем с цифровыми водяными знаками в рамках заданных ограничений // Захист інформації, 2002, №2. С. 58 – 65.* ***9****. Маракова И. И. Методика исследования секретных систем с цифровыми водяными знаками в условиях атаки в виде аддитивного шума и линейной фильтрацией // Захист інформації, 2003.– №4, С. 25 – 30.*

УДК 681.3

ВАРІАНТ ЗАВАДОСТІЙКОГО КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ

В'ячеслав Василенко
Відкрите акціонерне товариство "КП ОТІ"

Анотація: **Пропонується використання завадостійкого криптографічного перетворення для задач забезпечення конфіденційності інформаційних об'єктів автоматизованих систем.**
Summary: **Usage of noise-resistant cryptography conversion for problems of support of privacy of information objects of the automized systems is offered.**
Ключові слова: **Інформація, конфіденційність, криптографічні перетворення, завади, викривлення, відновлення.**

I Вступ

Забезпечення високої надійності, ефективності і технологічності автоматизованих систем (АС) можливо тільки за умови забезпечення високого рівня захищеності інформації, що циркулює в цих АС. Для цього відповідно до законів України про інформацію і її захист, а також відповідно до нормативних документів Системи технічного захисту інформації (ТЗІ) України в АС необхідним є застосування спеціальних засобів захисту, що призначаються для досягнення оптимального для даної АС об'єднання чотирьох **властивостей захищеності інформації автоматизованих систем** [1, 2, 3]: конфіденційності, цілісності, доступності і спостереженості. Залежно від умов застосування, складності і класу АС, а також характеристик можливих загроз вага цих функціональних властивостей може змінюватися, але проблеми забезпечення конфіденційності і цілісності інформації є одними з основних при розробці і впровадженні будь-яких захищених АС. При тому досить часто виникає задача одночасного забезпечення конфіденційності і цілісності одних і тих же інформаційних об'єктів. Причини цього можуть мати як суб'єктивний, так і об'єктивний характер.

Система ТЗІ забезпечує конфіденційність інформації, якщо вона зберігається, чи передається так, що сторонні (неавторизовані) користувачі не мають змоги отримати доступ до неї (при умові зберігання її у відкритому вигляді) [2] чи розкрити її смисловий зміст (при умові зберігання її у перетвореному вигляді) [4]. Звернемо увагу на те, що відсутність доступу до інформації не гарантує неможливість її отримання, наприклад завдяки витокам інформації технічними каналами. Окрім того, при зберіганні інформації у відкритому вигляді в багатокористувацьких АС можливе навмисне чи ненавмисне ознайомлення з конфіденційною інформацією тих авторизованих користувачів, для яких ця інформація не є призначеною. Отже в багатьох випадках криптографічне перетворення інформації є чи не єдиним шляхом забезпечення її конфіденційності (з певною стійкістю до спроб розкриття її змісту – криптографічною стійкістю). На цей час широко відомими є декілька алгоритмів криптографічного перетворення [4], із яких в Україні рекомендовано застосування алгоритму за ГОСТ 28147 – 89. При цьому деякі з алгоритмів криптографічного перетворення для зворотного перетворення потребують наявності лише невикривленої інформації, тобто інформації з гарантованою цілісністю.

В свою чергу, система ТЗІ забезпечує цілісність інформації [2], якщо вона зберігається, передається чи обробляється достовірною, повною і захищеною від ненавмисних і навмисних викривлень. Одним з основних способів забезпечення цілісності інформації в автоматизованих системах є застосування засобів контролю цілісності інформаційних об'єктів з її подальшім відновленням. Не зупиняючись на причинах